

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

<http://www.us-cert.gov/tlp/>

**DATE(S) ISSUED:**

09/13/2016

**SUBJECT:**

Multiple Vulnerabilities in Microsoft Graphics Component Could Allow for Remote Code Execution (MS16-106)

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Microsoft's Graphics Component, which could allow for remote code execution. These vulnerabilities can be exploited by either convincing a user to open a specially crafted document or visit a specially crafted webpage. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

**THREAT INTELLIGENCE:**

There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEMS AFFECTED:**

- Microsoft Windows Vista, 7, 8.1, RT 8.1, 10
- Microsoft Windows Server 2008 and 2008 R2 (Including Server Core Installations)
- Microsoft Windows Server 2012 and 2012 R2 (including Server Core Installations)

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **Medium**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **Medium**

**Home users: Low**

**TECHNICAL SUMMARY:**

Multiple vulnerabilities have been discovered in Microsoft's Graphics Component, the worst of which could allow for remote code execution. The vulnerabilities are as follows:

- A remote code execution vulnerability exists in the way Windows Graphic Device Interface handles objects in memory (CVE-2016-3356).
- Three elevation of privilege vulnerabilities exist in the way Windows handles objects in memory (CVE-2016-3348, CVE-2016-3349, CVE-2016-3355).
- An information disclosure vulnerability exists in the way the Windows Graphics Device Interface handles objects in memory (CVE-2016-3354).

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

#### **RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

#### **REFERENCES:**

##### **Microsoft:**

<https://technet.microsoft.com/en-us/library/security/ms16-106.aspx>

##### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3348>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3349>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3354>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3355>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3356>

#### **TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

<http://www.us-cert.gov/tlp/>